--8--

REMARKS

Claims 1, 3-10, 13-19, and 21-25 are currently pending in the application. By this response, no claims are amended or added for the Examiner's consideration. Reconsideration of the rejected claims in view of the following remarks is respectfully requested.

35 U.S.C. §103 Rejection

Claims 1, 3-5, 8-10, 13 ,14, and 22

Claims 1, 3-5, 8-10, 13 ,14, and 22 were rejected under 35 U.S.C. §103(a) for being unpatentable over U.S. Patent No. 7,024,690 issued to Young, et al. ("Young") in view of U.S. Patent No. 5,497,421 issued to Kaufman, et al. ("Kaufman") in further view of U.S. Patent No. 6,539,482 issued to Blanco, et al. ("Blanco"). This rejection is respectfully traversed.

The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness. To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings.[1] Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed

---

[1] While the *KSR* court rejected a rigid application of the teaching, suggestion, or motivation ("TSM") test in an obviousness inquiry, the [Supreme] Court acknowledged the importance of identifying "a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does" in an obviousness determination. *Takeda Chemical Industries, Ltd. v. Alphapharm Pty., Ltd.*, 492 F.3d 1350, 1356-1357 (Fed. Cir. 2007) (quoting *KSR International Co. v. Teleflex Inc.*, --- U.S. ----, 127 S.Ct. 1727, 1731 (2007)).

combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP §2142. Applicants submit that no proper combination of the applied art teaches or suggests each and every feature of the claimed invention.

> *Independent Claims 1, 9, and 22*

Claim 1 recites, in pertinent part:

> ... creating a credential string on a portal server, the credential string being an encrypted hash of a session ID;
> sending a UserID associated with the session ID and the credential string to a software application from the portal server, while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server;
> receiving a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, the confirmation request including the credential string...

Claim 9 recites, in pertinent part:

> ... receiving a UserID and a credential string at an authentication proxy server, the credential string being an encrypted hash of a session ID, which is created at a portal;
> sending a confirmation request from the authentication proxy to the portal while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal, the confirmation request includes the credential string;
> receiving a response at the authentication proxy for the confirmation request while maintaining the user password on the portal such that the user password is not required to authenticate the User ID...

Claim 22 recites, in pertinent part:

> ... create a credential string on a portal server, the credential string being an encrypted hash of a session ID;

> send a UserID associated with the session ID and the credential string to a software application from the portal server, while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server;
> receive a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, the confirmation request including the credential string...

Applicants agree with the Examiner's assertion on page 3 of the Office Action, wherein the Examiner recognizes that Young fails to maintain the user password on the portal and avoids exposing the user password to network resources beyond the portal. However, Applicants submit that Kaufman fails to make up for this deficiency. Instead, Kaufman creates two separate hash values (H1 and H2) of the user's password (P). These hash values of the password are created on a user workstation 12. (See Figs. 4 and 5; Col. 6, lines 42-44.) Young uses the login agent's public key (LA-PUB) to encrypt H2 along with a randomly generated secret nonce key K. Young combines the user name N with encrypted H2 and K to create a message M. This message, which includes a hashed version of the password H2, is sent to the login agent 26. (Col. 7, lines 25-44; Figs. 4 and 5.)

The login agent parses out the username N and sends it to a certificate storage server (CSS) 24. The CSS uses the username N to find the user's encrypted credentials {U}H1, which is an encryption of H1 and the user's private RSA key U. Young appends the encrypted credential {U}H1 to H2 and encrypts the combination using the login agent's public key (LA-PUB) to form a doubly encrypted credential D. (Col. 6, lines 51-60.) This doubly encrypted credential D, which contains hashed passwords H1 and H2, is sent to the login agent 26. (Col. 7, lines 44-56; See Fig. 3.) As such, Young uses a variety of hashing and encryption mechanisms to protect the user's password before the password is sent from the user's workstation to a login agent, from the login agent to a CSS, and from the CSS back to the login agent, etc. However, despite these hashing and encryption mechanisms, Young still exposes the

user's password to a variety of network resources. As such, Applicants submit Young does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

Applicants further submit that Blanco does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. Instead, Blanco includes an authentication system, which includes a directory service containing a remote access password and a standard access password for each user of the network. Blanco uses an authentication protocol that provides information on whether a user is accessing the network locally or remotely, and includes a front-end between the directory service and the authentication protocol. The front-end receives a user identifier and a user password entered by a user through the authentication protocol, and retrieves from the directory service the remote access password and the standard access password corresponding to the user identifier. If the authentication protocol indicates a remote access, the front-end compares the user password to the remote access password, else it compares the user password to the standard access password. Access to the network is granted if the comparison is successful. (Abstract; See, e.g., Fig. 2.) Therefore, Blanco does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. As such, Applicants submit claims 1, 9, and 22 are not obvious and respectfully request the rejection of claims 1, 9, and 22 be withdrawn.

Dependent Claims 3-5, 8, 10, 13, and 14

Claims 3-5, 8, 10, 13, and 14 are dependent claims, depending on respective independent claims 1 and 9. For this reason, Applicants submit that these claims are thus distinguishable based on independent claims 1 and 9, respectively. Accordingly, Applicants respectfully request the rejection over claims 3-5, 8, 10, 13, and 14 be withdrawn.

Claims 6, 7, 15, 19, and 23-25

Claims 6, 7, 15, 19, and 23-25 were rejected under 35 U.S.C. §103(a) for being unpatentable over Young in view of Kaufman in further view of U.S. Patent No. 7,100,054 issued to Wenisch, et al. ("Wenisch"). This rejection is respectfully traversed.

Independent Claim 15

Claim 15 recites, in pertinent part:

> ... wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal.

Applicants agree with the Examiner's assertion on page 7 of the Office Action that Young does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. However, Applicants submit that neither Kaufman nor Wenisch maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

As described above, Kaufman uses a variety of hashing and encryption mechanisms to protect the user's password before the password is sent from the user's workstation to a login agent, from the login agent to a CSS, and from the CSS back to the login agent, etc. However, despite these hashing and encryption mechanisms, Kaufman still exposes the user's password to a variety of network resources. As such, Applicants submit Kaufman does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

Applicants further submit that Wenisch does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. Instead, Wenisch allows a user to log into a computer. Information from the login, including the user's password and username, are sent to a web server via a login

packet. The web server encrypts the password and username and sends it to an authentication provider. (See Fig. 2; Col. 3, line15 – Col. 4, line 35.) Therefore, Wenisch sends a password from a computer to a web server and to an authentication provider. However, Wenisch does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. Accordingly, Applicants respectfully request the rejection of claim 15 be withdrawn.

Dependent Claims 6, 7, 19, and 23-25

Claims 6, 7, 19, and 23-25 are dependent claims, depending on respective independent claims 1, 15, and 22. For this reason, Applicants submit that these claims are thus distinguishable based on independent claims 1, 15, and 22, respectively. Accordingly, Applicants respectfully request the rejection over claims 6, 7, 19, and 23-25 be withdrawn.

Claims 16-18 and 21

Claims 16-18 and 21 were rejected under 35 U.S.C. §103(a) for being unpatentable over Young in view of Kaufman, Wenisch, and Blanco. This rejection is respectfully traversed.

Claims 16-18 and 21 are dependent claims, depending on independent claim 15. For this reason, Applicants submit that these claims are thus distinguishable based on independent claim 15. Accordingly, Applicants respectfully request the rejection over claims 16-18, and 21 be withdrawn.
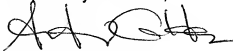
CONCLUSION

In view of the foregoing amendments and remarks, Applicants submit that all of the claims are patentably distinct from the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to

issue. The Examiner is invited to contact the undersigned at the telephone number listed below, if needed. Applicants hereby makes a written conditional petition for extension of time, if required. Please charge any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 09-0457.

Respectfully submitted,

Andrew M. Calderon
Registration No. 38,093

Greenblum & Bernstein, P.L.C.
1950 Roland Clarke Place
Reston, Virginia 20191
Telephone: 703-716-1191
Facsimile: 703-716-1180